南明离火
移动应用检测平台

# ANDROID 静态分析报告

薪分期. • v4.1.2

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

分析日期: 2025-07-06 20:27:28

# 应用概览

| | |
|---|---|
| 文件名称: | 薪分期.apk |
| 文件大小: | 16.07MB |
| 应用名称: | 薪分期. |
| 软件包名: | ysvwpx.tmdfkzeatpwid.ztfbxxbeekxakdjl |
| 主活动: | com.xinfenq.ui.activitys.JDXF0ACT |
| 版本号: | 4.1.2 |
| 最小SDK: | 22 |
| 目标SDK: | 28 |
| 加固信息: | 未加壳 |
| 开发框架: | Java/Kotlin |
| 应用程序安全分数: | 46/100 (中风险) |
| 杀软检测: | 11 个杀毒软件报毒 |
| MD5: | abc422f35dc877fcf23aa5c7cd08c465 |
| SHA1: | fa9ffec7c4915fc3d780aa496bb09f069e537142 |
| SHA256: | 07218054c69484fae3d9d393bd146879939820fb0cfb05e8ceb7c1b9eb22c174 |

# 恶意软件家族情报

| | |
|---|---|
| 恶意家族 | 开通会员：查看恶意软件家族归属 |
| 描述信息 | 升级会员：解锁高级权限 |
| C2服务器 | 升级会员：解锁高级权限 |
| 凭证数据 | 升级会员：解锁高级权限 |
| 关联情报 | 升级会员：解锁高级权限 |

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

# 分析结果严重性分布

| 高危 | 中危 | 信息 | 安全 | 关注 |
| --- | --- | --- | --- | --- |
| 4 | 11 | 2 | 2 | 4 |

## 四大组件导出状态统计

| |
| --- |
| Activity组件：342个，其中export的有： 0个 |
| Service组件：1个，其中export的有： 0个 |
| Receiver组件：2个，其中export的有： 2个 |
| Provider组件：3个，其中export的有： 0个 |

## 应用签名证书信息

APK已签名
v1 签名: True
v2 签名: True
v3 签名: True
v4 签名: False
主题: C=niTXFuuh, ST=JTKNFTss, L=VPTOCAeC, O=FpVWZgSA, OU=WicswEiS, CN=RNcUNLWk
签名算法: rsassa_pkcs1v15
有效期自: 2025-01-07 16:57:04+00:00
有效期至: 2035-01-05 16:57:04+00:00
发行人: C=niTXFuuh, ST=JTKNFTss, L=VPTOCAeC, O=FpVWZgSA, OU=WicswEiS, CN=RNcUNLWk
序列号: 0x2d38184ce33a703b
哈希算法: sha256
证书MD5: b59f48e790944b89a195791530d56e30
证书SHA1: aca5474f60864bc497cfa7fd27a6bbacd42c61dc
证书SHA256: 4024abe63cbc492530a5247c997706e13[illegible]e27436cae151466b0a[illegible]d2
证书SHA512:
54a71836b0d5cbd371c196c65755a8d54ff17[illegible]7794a98e8076c59[illegible]8c6df4e57e4e7171e5b80bd450e326bfe4bedf1c68a1b3f44afde49517b

公钥算法: rsa
密钥长度: 2048
指纹: 9c6f3c7c0713182787bf2220[illegible]f833e0af522376879[illegible]fbca2c7c5
共检测到 1 个唯一证书

## 权限声明与风险分级

| 权限名称 | 安全等级 | 权限内容 | 权限描述 |
| --- | --- | --- | --- |
| android.permission.INTERNET | 危险 | 完全互联网访问 | 允许应用程序创建网络套接字。 |
| android.permission.ACCESS_WIFI_STATE | 普通 | 查看Wi-Fi状态 | 允许应用程序查看有关Wi-Fi状态的信息。 |
| android.permission.CHANGE_WIFI_STATE | 危险 | 改变Wi-Fi状态 | 允许应用程序改变Wi-Fi状态。 |
| android.permission.READ_PHONE_STATE | 危险 | 读取手机状态和标识 | 允许应用程序访问设备的手机功能。有此权限的应用程序可确定此手机的号码和序列号，是否正在通话，以及对方的号码等。 |

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

| | | | |
|---|---|---|---|
| android.permission.WRITE_EXTERNAL_STORAGE | 危险 | 读取/修改/删除外部存储内容 | 允许应用程序写入外部存储。 |
| android.permission.WRITE_CONTACTS | 危险 | 写入联系人信息 | 允许应用程序修改您手机上存储的联系人（地址）数据。恶意应用程序可借此清除或修改您的联系人数据。 |
| android.permission.READ_CONTACTS | 危险 | 读取联系人信息 | 允允许应用程序读取您手机上存储的所有联系人（地址）数据。恶意应用程序可借此将您的数据发送给其他人。 |
| android.permission.READ_SMS | 危险 | 读取短信 | 允许应用程序读取您的手机或 SIM 卡中存储的短信。恶意应用程序可借此读取您的机密信息。 |
| android.permission.CAMERA | 危险 | 拍照和录制视频 | 允许应用程序拍摄照片和视频，且允许应用程序收集相机在任何时候拍到的图像。 |
| android.permission.WRITE_CALL_LOG | 危险 | 写入通话记录 | 允许应用程序写入（但不读取）用户的通话记录数据。 |
| android.permission.READ_CALL_LOG | 危险 | 读取通话记录 | 允许应用程序读取用户的通话记录 |
| android.permission.ACCESS_NETWORK_STATE | 普通 | 获取网络状态 | 允许应用程序查看所有网络的状态。 |
| android.permission.READ_EXTERNAL_STORAGE | 危险 | 读取SD卡内容 | 允许应用程序从SD卡读取信息。 |
| android.permission.RECORD_AUDIO | 危险 | 获取录音权限 | 允许应用程序获取录音权限。 |
| android.permission.CHANGE_NETWORK_STATE | 危险 | 改变网络连通性 | 允许应用程序改变网络连通性。 |
| android.permission.REQUEST_INSTALL_PACKAGES | 危险 | 允许安装应用程序 | Android8.0以上系统允许安装未知来源应用程序权限。 |
| android.permission.READ_MEDIA_VISUAL_USER_SELECTED | 危险 | 允许从外部存储读取用户选择的图像或视频文件 | 允许应用程序从用户通过权限提示照片选择器选择的外部存储中读取图像或视频文件。应用程序可以检查此权限以验证用户是否决定使用照片选择器，而不是授予对 READ_MEDIA_IMAGES 或 READ_MEDIA_VIDEO 的访问权限。它不会阻止应用程序手动访问标准照片选择器。应与 READ_MEDIA_IMAGES 和/或 READ_MEDIA_VIDEO 一起请求此权限，具体取决于所需的媒体类型。 |
| android.permission.READ_MEDIA_IMAGES | 危险 | 允许从外部存储读取图像文件 | 允许应用程序从外部存储读取图像文件。 |
| android.permission.READ_MEDIA_VIDEO | 危险 | 允许从外部存储读取视频文件 | 允许应用程序从外部存储读取视频文件。 |
| android.permission.READ_MEDIA_AUDIO | 危险 | 允许从外部存储读取音频文件 | 允许应用程序从外部存储读取音频文件。 |

## 网络通信安全风险分析

| 序号 | 范围 | 严重级别 | 描述 |
|---|---|---|---|

## 证书安全合规分析

高危: **0** | 警告: **1** | 信息: **1**

本报告由南明离火移动安全分析平台生成

| 标题 | 严重程度 | 描述信息 |
| --- | --- | --- |
| 已签名应用 | 信息 | 应用已使用代码签名证书进行签名。 |

## Manifest 配置安全分析

高危: **0** | 警告: **3** | 信息: **0** | 屏蔽: **0**

| 序号 | 问题 | 严重程度 | 描述信息 |
| --- | --- | --- | --- |
| 1 | 应用已启用明文网络流量 [android:usesCleartextTraffic=true] | 警告 | 应用允许明文网络流量（如 HTTP、FTP 协议、DownloadManager、MediaPlayer 等）。API 级别 27 及以下默认启用，28 及以上默认禁用。明文流量缺乏机密性、完整性和真实性保护，攻击者可窃听或篡改传输数据。建议关闭明文流量，仅使用加密协议。 |
| 2 | Broadcast Receiver (com.base.commonlibrary.netstate.NetworkStateReceiver) 未受保护。<br>存在 intent-filter。 | 警告 | 检测到 Broadcast Receiver 已与设备上的其他应用共享，因此可被任意应用访问。intent-filter 的存在表明该 Broadcast Receiver 被显式导出，存在安全风险。 |
| 3 | Broadcast Receiver (com.xinfenq.gzd.FZGBReceiver) 未受保护。<br>存在 intent-filter。 | 警告 | 检测到 Broadcast Receiver 已与设备上的其他应用共享，因此可被任意应用访问。intent-filter 的存在表明该 Broadcast Receiver 被显式导出，存在安全风险。 |

## 代码安全漏洞检测

高危: **4** | 警告: **7** | 信息: **2** | 安全: **1** | 屏蔽: **0**

| 序号 | 问题 | 等级 | 参考标准 | 文件位置 |
| --- | --- | --- | --- | --- |
| 1 | 应用程序记录日志信息,不得记录敏感信息 | 信息 | CWE: CWE-532: 通过日志文件的信息暴露<br>OWASP MASVS: MSTG-STORAGE-3 | 升级会员：解锁高级权限 |
| 2 | 应用程序可以读取/写入外部存储器，任何应用程序都可以读取写入外部存储器的数据 | 警告 | CWE: CWE-276: 默认权限不正确<br>OWASP Top 10: M2: Insecure Data Storage<br>OWASP MASVS: MSTG-STORAGE-2 | 升级会员：解锁高级权限 |
| 3 | 文件可能包含硬编码的敏感信息，如用户名、密码、密钥等 | 警告 | CWE: CWE-312: 明文存储敏感信息<br>OWASP Top 10: M9: Reverse Engineering<br>OWASP MASVS: MSTG-STORAGE-14 | 升级会员：解锁高级权限 |

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

| | | | | |
|---|---|---|---|---|
| 4 | 应用程序创建临时文件。敏感信息永远不应该被写进临时文件 | 警告 | CWE: CWE-276: 默认权限不正确<br>OWASP Top 10: M2: Insecure Data Storage<br>OWASP MASVS: MSTG-STORAGE-2 | 升级会员：解锁高级权限 |
| 5 | 应用程序使用不安全的随机数生成器 | 警告 | CWE: CWE-330: 使用不充分的随机数<br>OWASP Top 10: M5: Insufficient Cryptography<br>OWASP MASVS: MSTG-CRYPTO-6 | 升级会员：解锁高级权限 |
| 6 | SHA-1是已知存在哈希冲突的弱哈希 | 警告 | CWE: CWE-327: 使用了破损或被认为是不安全的加密算法<br>OWASP Top 10: M5: Insufficient Cryptography<br>OWASP MASVS: MSTG-CRYPTO-4 | 升级会员：解锁高级权限 |
| 7 | MD5是已知存在哈希冲突的弱哈希 | 警告 | CWE: CWE-327: 使用了破损或被认为是不安全的加密算法<br>OWASP Top 10: M5: Insufficient Cryptography<br>OWASP MASVS: MSTG-CRYPTO-4 | 升级会员：解锁高级权限 |
| 8 | 不安全的Web视图实现。Web视图忽略SSL证书错误并接受任何SSL证书。此应用程序易受MITM攻击 | 高危 | CWE: CWE-295: 证书验证不恰当<br>OWASP Top 10: M3: Insecure Communication<br>OWASP MASVS: MSTG-NETWORK-3 | 升级会员：解锁高级权限 |
| 9 | 已启用远程WebView调试 | 高危 | CWE: CWE-919: 移动应用程序中的弱点<br>OWASP Top 10: M1: Improper Platform Usage<br>OWASP MASVS: MSTG-RESILIENCE-2 | 升级会员：解锁高级权限 |
| 10 | 该文件是World Writable。任何应用程序都可以写入文件 | 高危 | CWE: CWE-276: 默认权限不正确<br>OWASP Top 10: M2: Insecure Data Storage<br>OWASP MASVS: MSTG-STORAGE-2 | 升级会员：解锁高级权限 |

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

| | | | | |
|---|---|---|---|---|
| 11 | 此应用程序将数据复制到剪贴板。敏感数据不应复制到剪贴板，因为其他应用程序可以访问它 | 信息 | OWASP MASVS: MSTG-STORAGE-10 | 升级会员：解锁高级权限 |
| 12 | 不安全的Web视图实现。可能存在WebView任意代码执行漏洞 | 警告 | CWE: CWE-749: 暴露危险方法或函数<br>OWASP Top 10: M1: Improper Platform Usage<br>OWASP MASVS: MSTG-PLATFORM-7 | 升级会员：解锁高级权限 |
| 13 | 此应用程序使用SSL Pinning 来检测或防止安全通信通道中的MITM攻击 | 安全 | OWASP MASVS: MSTG-NETWORK-4 | 升级会员：解锁高级权限 |
| 14 | 如果一个应用程序使用WebView.loadDataWithBaseURL方法来加载一个网页到WebView，那么这个应用程序可能会遭受跨站脚本攻击 | 高危 | CWE: CWE-79: 在Web页面生成时对输入的转义处理不恰当（'跨站脚本'）<br>OWASP Top 10: M1: Improper Platform Usage<br>OWASP MASVS: MSTG-PLATFORM-6 | 升级会员：解锁高级权限 |

## Native 库安全加固检测

| 序号 | 动态库 | NX(堆栈禁止执行) | PIE | STACK CANARY(栈保护) | RELRO | RPATH（指定SO搜索路径） | RUNPATH（指定SO搜索路径） | FORTIFY(常用函数加强检查) | SYMBOLS STRIPPED(裁剪符号表) |
|---|---|---|---|---|---|---|---|---|---|

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 1 | arm64-v8a/libfacedevice.so | True<br>info<br>二进制文件设置了 NX 位。这标志着内存页面不可执行，使得攻击者注入的 shellcode 不可执行。 | 动态共享对象 (DSO)<br>info<br>共享库是使用 -fPIC 标志构建的，该标志启用与地址无关的代码。这使得面向返回的编程（ROP）攻击更难可靠地执行。 | True<br>info<br>这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出 | Full RELRO<br>info<br>此共享对象已完全启用 RELRO。RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT（.got 和 .got.plt 两者）被标记为只读。 | None<br>info<br>二进制文件没有设置运行时搜索路径或 RPATH | None<br>info<br>二进制文件没有设置 RUNPATH | True<br>info<br>二进制文件有以下加固函数: ['__vsprintf_chk', '__memmove_chk', '__strchr_chk', '__memset_chk', '__memcpy_chk', '__strcpy_chk', '__vsnprintf_chk', '__strlen_chk'] | True<br>info<br>符号被剥离 |
| 2 | arm64-v8a/libtoyger.so | True<br>info<br>二进制文件设置了 NX 位。这标志着内存页面不可执行，使得攻击者注入的 shellcode 不可执行。 | 动态共享对象 (DSO)<br>info<br>共享库是使用 -fPIC 标志构建的，该标志启用与地址无关的代码。这使得面向返回的编程（ROP）攻击更难可靠地执行。 | True<br>info<br>这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出 | Full RELRO<br>info<br>此共享对象已完全启用 RELRO。RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT（.got 和 .got.plt 两者）被标记为只读。 | None<br>info<br>二进制文件没有设置运行时搜索路径或 RPATH | None<br>info<br>二进制文件没有设置 RUNPATH | False<br>warning<br>二进制文件没有任何加固函数。加固函数提供了针对 glibc 的常见不安全函数（如 strcpy，gets 等）的缓冲区溢出检查。使用编译选项 -D_FORTIFY_SOURCE=2 来加固函数。这个检查对于 Dart/Flutter 库不适用 | True<br>info<br>符号被剥离 |

## 应用行为分析

| 编号 | 行为 | 标签 | 文件 |
|---|---|---|---|
| 00013 | 读取文件并将其放入流中 | 文件 | 升级会员：解锁高级权限 |

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

| | | | |
|---|---|---|---|
| 00054 | 从文件安装其他APK | 反射 | 升级会员：解锁高级权限 |
| 00063 | 隐式意图（查看网页、拨打电话等） | 控制 | 升级会员：解锁高级权限 |
| 00022 | 从给定的文件绝对路径打开文件 | 文件 | 升级会员：解锁高级权限 |
| 00036 | 从 res/raw 目录获取资源文件 | 反射 | 升级会员：解锁高级权限 |
| 00091 | 从广播中检索数据 | 信息收集 | 升级会员：解锁高级权限 |
| 00014 | 将文件读入流并将其放入 JSON 对象中 | 文件 | 升级会员：解锁高级权限 |
| 00125 | 检查给定的文件路径是否存在 | 文件 | 升级会员：解锁高级权限 |
| 00033 | 查询IMEI号 | 信息收集 | 升级会员：解锁高级权限 |
| 00192 | 获取短信收件箱中的消息 | 短信 | 升级会员：解锁高级权限 |
| 00051 | 通过setData隐式意图（查看网页、拨打电话等） | 控制 | 升级会员：解锁高级权限 |
| 00191 | 获取短信收件箱中的消息 | 短信 | 升级会员：解锁高级权限 |
| 00096 | 连接到 URL 并设置请求方法 | 命令<br>网络 | 升级会员：解锁高级权限 |
| 00072 | 将 HTTP 输入流写入文件 | 命令<br>网络<br>文件 | 升级会员：解锁高级权限 |
| 00089 | 连接到 URL 并接收来自服务器的输入流 | 命令<br>网络 | 升级会员：解锁高级权限 |
| 00030 | 通过给定的 URL 连接到远程服务器 | 网络 | 升级会员：解锁高级权限 |
| 00094 | 连接到 URL 并从中读取数据 | 命令<br>网络 | 升级会员：解锁高级权限 |
| 00108 | 从给定的 URL 读取输入流 | 网络<br>命令 | 升级会员：解锁高级权限 |
| 00147 | 获取当前位置的时间 | 信息收集<br>位置 | 升级会员：解锁高级权限 |
| 00075 | 获取设备的位置 | 信息收集<br>位置 | 升级会员：解锁高级权限 |
| 00115 | 获取设备的最后已知位置 | 信息收集<br>位置 | 升级会员：解锁高级权限 |
| 00202 | 打电话 | 控制 | 升级会员：解锁高级权限 |
| 00203 | 将电话号码放入意图中 | 控制 | 升级会员：解锁高级权限 |
| 00173 | 获取 AccessibilityNodeInfo 屏幕中的边界并执行操作 | 无障碍服务 | 升级会员：解锁高级权限 |
| 00002 | 打开相机并拍照 | 相机 | 升级会员：解锁高级权限 |
| 00183 | 获取当前相机参数并更改设置 | 相机 | 升级会员：解锁高级权限 |

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

| | | | |
|---|---|---|---|
| 00034 | 查询当前数据网络类型 | 信息收集<br>网络 | 升级会员：解锁高级权限 |
| 00077 | 读取敏感数据（短信、通话记录等） | 信息收集<br>短信<br>通话记录<br>日历 | 升级会员：解锁高级权限 |
| 00109 | 连接到 URL 并获取响应代码 | 网络<br>命令 | 升级会员：解锁高级权限 |

## 敏感权限滥用分析

| 类型 | 匹配 | 权限 |
|---|---|---|
| 恶意软件常用权限 | 9/30 | android.permission.READ_PHONE_STATE<br>android.permission.WRITE_CONTACTS<br>android.permission.READ_CONTACTS<br>android.permission.READ_SMS<br>android.permission.CAMERA<br>android.permission.WRITE_CALL_LOG<br>android.permission.READ_CALL_LOG<br>android.permission.RECORD_AUDIO<br>android.permission.REQUEST_INSTALL_PACKAGES |
| 其它常用权限 | 10/46 | android.permission.INTERNET<br>android.permission.ACCESS_WIFI_STATE<br>android.permission.CHANGE_WIFI_STATE<br>android.permission.WRITE_EXTERNAL_STORAGE<br>android.permission.ACCESS_NETWORK_STATE<br>android.permission.READ_EXTERNAL_STORAGE<br>android.permission.CHANGE_NETWORK_STATE<br>android.permission.READ_MEDIA_IMAGES<br>android.permission.READ_MEDIA_VIDEO<br>android.permission.READ_MEDIA_AUDIO |

常用: 已知恶意软件广泛滥用的权限。

其它常用权限: 已知恶意软件经常滥用的权限。

## 恶意域名威胁检测

| 域名 | 状态 | 中国境内 | 位置信息 |
|---|---|---|---|
| jzlwjfanjzxcv.s3.ap-east-1.amazonaws.com | 安全 | 是 | **IP**地址: 52.95.162.74<br>国家: 中国<br>地区: 香港<br>城市: 香港<br>纬度: 22.285521<br>经度: 114.157692<br>查看: 高德地图 |
| www.beizhuabao.com | 安全 | 否 | No Geolocation information available. |

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

| | | | |
|---|---|---|---|
| zcvkjliuoqwead-1329567725.cos.ap-guangzhou.myqcloud.com | 安全 | 是 | **IP地址:** 27.155.119.148<br>国家: 中国<br>地区: 福建<br>城市: 福州<br>纬度: 26.061390<br>经度: 119.306107<br>查看: 高德地图 |
| ijljlkjzxcv-1324028813.cos.ap-guangzhou.myqcloud.com | 安全 | 是 | **IP地址:** 27.155.119.140<br>国家: 中国<br>地区: 福建<br>城市: 福州<br>纬度: 26.061390<br>经度: 119.306107<br>查看: 高德地图 |
| nice800.com | 安全 | 是 | **IP地址:** 45.122.110.135<br>国家: 中国<br>地区: 香港<br>城市: 香港<br>纬度: 22.285521<br>经度: 114.157692<br>查看: 高德地图 |

## URL 链接安全分析

| URL信息 | 源码文件 |
|---|---|
| • https://android-donwload.oss-cn-hangzhou.aliyuncs.com/d[illegible]sfnname/5100sdfh0[illegible]t/ | c/k/b/d/a/d.java |
| • https://ijljlkjzxcv-1324028813.cos.ap-guangzhou.myqcloud.com<br>• https://zcvkjliuoqwead-1329567725.cos.ap-guangzhou.myqcloud.com<br>• https://jzlwjfanjzxcv.s3.ap-east-1.amazonaws.com | c/k/b/d/a/e.java |
| • http://www.beizhuabao.com | c/k/b/d/a/a.java |
| • https://nice800.com/ | com/xinfenq/ui/activitys/MT10ACT.java |
| • http://www.beizhuabao.com | c/k/b/d/a/b.java |
| • https://nice800.com | com/xinfenq/ui/activitys/MT7ACT.java |
| • https://tianshu.alicdn.com/7504f3f0-a[illegible]-4636-b486-e396559d3efb.png<br>• https://cn-shanghai-aliyun-cloudauth-oss.cn-shanghai.aliyuncs.com/model/toyger.face.dat | c/f/a/n/k.java |
| • https://render.alipay.com/p/yuyan/180020010001208736/aliyunfacewelcome.html | 自研引擎-S |

## 第三方 SDK 组件分析

| SDK名称 | 开发者 | 描述信息 |
|---|---|---|
| 金融级实人认证 SDK | Alibaba | 金融级实人认证服务搭载真人检测和人脸比对等生物识别技术，配合权威数据源验证，可快速校验自然人的真实身份。 |
| C++ 共享库 | Android | 在 Android 应用中运行原生代码。 |

本报告由南明离火移动安全分析平台生成

| | | |
|---|---|---|
| AgentWeb | Justson | AgentWeb 是一个基于的 Android WebView，极度容易使用以及功能强大的库，提供了 Android WebView 一系列的问题解决方案，并且轻量和极度灵活。 |
| File Provider | Android | FileProvider 是 ContentProvider 的特殊子类，它通过创建 content://Uri 代替 file:///Uri 以促进安全分享与应用程序关联的文件。 |

## 敏感凭证泄露检测

| 可能的密钥 |
|---|
| 凭证信息=> "com.amap.com.xinfenq.mjyp.app.api.v2.apikey" : "0bsdfvdd0" |
| b20292cc45269854c712 |
| b48852f124ad471e9b6ad06066c50e65 |
| 7504f3f0-aca8-4636-b486-e396559d3efb |
| fd4ddd72c85fd5fe2913be520df32ed0 |
| ab05c5fe1172477aa023e3046a6abbd2 |
| 09ce2f7bfb9243debf2c2efe05a1d047 |
| MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC3DtFIIG5OhLgYu4M3CAx4DAhLyag2HSd2lsr1166nH9SdefhaknsujWnumk+yNMYlQFdDnJ1Z8A4kj6zLJYRnNLyUeU0tI9uMlPr6AGbdiaV85BoK0YXJY6pxEw3w55oozhTjMswJRyv93o8fBKWx/7mAhsrayE8VITzHroIuQIDAQAB |
| f4qgkb85q4pMRMChLeC7uSn2wwTWGXrs |

## 免责声明及风险提示:

本报告由南明离火移动安全分析平台自动生成，内容仅供参考，不构成任何法律意见或建议。本平台对使用本产品及其内容所引发的任何直接或间接损失概不负责。本报告内容仅供网络安全研究，不得违反中华人民共和国相关法律法规。如有任何疑问，请及时与我们联系。

南明离火移动安全分析平台是一款专业的移动端恶意软件分析和安全评估框架。它能够执行静态分析和动态分析，深入扫描软件中中潜在的漏洞和安全隐隐患。

© 2025 南明离火 - 移动安全分析平台自动生成

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成